

REMARKS/ARGUMENTS

Claims 1-28 and 33-34 are pending in the present application. Claims 1, 4, 7, 10, 13, 17, 21 and 25 are independent claims.

Reply to Examiner's Response to Arguments

Since the Examiner has maintained the prior rejections and has provided arguments in support of this position, Applicant will address the Examiner's response first.

1. The Examiner's arguments related to the 35 U.S.C. § 103(a) rejection based on Barnett does not address claim language argued by Applicant as distinguishing over each applied reference.

Based on Applicant's review of the Examiner's Response to Arguments section presented in the 12/15/2008 Final Rejection, Applicant believes that the Examiner has misinterpreted the arguments made by Applicant in the Amendment filed on 9/25/2008.

As an initial matter, the Examiner and Applicant are in agreement in that Alden (6,101,543) and Citta (4,771,458) do not disclose "using a sequential code for which a unique key is derived for encrypting the data" (e.g., see Page 4 of the 12/15/2008 Final Rejection). The Examiner cites to Barnett (6,661,896) for allegedly disclosing this limitation based on Barnett's disclosure related to a character string.

In the Amendment of 9/25/2008, Applicant attempted to show that *even assuming* that the Examiner was correctly interpreting Barnett's character string as a "sequential code", Barnett remains deficient because the character string in Barnett is never encapsulated in a transport

Reply to Office Action dated December 15, 2008

frame, and as such Barnett is not combinable with Alden and/or Citta to achieve the limitation, emphasized below, of “encrypting a first data frame based on a first unique code in a first communication device, said first unique code being derived from a first sequential code “ and “encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code” as recited in independent claim 1, for example (emphasis added).

At best, while not an admission on the part of Applicant, the Examiner has merely shown that Barnett teaches using a predetermined character string to encrypt a packet. Upon encrypting the packet, however, Barnett does not disclose or suggest encapsulating the encrypted packet in a frame that also includes the predetermined character string.

As discussed in Applicant’s previous response, in Barnett, a character string is input by a user at a workstation, and is then used to compute a transport key and a unique key (e.g., see Col. 3, lines 53-55 of Barnett). A data packet is then encrypted at the workstation, and the data packet is sent to a server along with the transport key (e.g., see Col. 3, lines 56-60 of Barnett). The server then compares the transport key with a predefined list of transport keys maintained at the server, loads the unique encryption key corresponding to a matching transport key from the list and decrypts the packet based on the unique encryption key (e.g., See Barnett at Col. 3, lines 59-67, also see “*If the transport key is not in the predefined list of transport keys, the packet is discarded. If the transport key is in the list, the packet is decrypted using the encryption key within the table*” at Col. 5, lines 2-6 of Barnett). **Clearly, the character string is not included in a frame along with the encrypted packet; rather, only the transport key is included.**

The Examiner’s response to the arguments presented above was that Barnett was only intended to “show that a unique encryption code is generated based on sequential code” (e.g., see Page 3 of the 12/15/2008 Final rejection). However, this does not address that the claim

language that recites portions of the “sequential code” to be included in the transport frame. There is no such disclosure within Barnett for the reasons expressed above. The Examiner cannot simply ignore the claim language of “encapsulating said first encrypted data frame in a first transport frame, said *first transport frame comprising a first portion and a second portion of said first sequential code*” as recited in independent claim 1 (emphasis added). Because it is acknowledged that Alden and Citta are silent regarding the “sequential code” as claimed, and the feature of Barnett read upon by the “sequential code” is not included in a transport frame, the combination of Alden, Citta and Barnett is deficient.

Applicant respectfully submits that the remaining independent claims 4, 7, 10, 13, 17, 21 and 25 include similar claim language as that addressed above, and are allowable for the same reasons.

1. The Examiner’s comments in the 12/15/2008 Final Rejection do not address Applicant’s arguments regarding the combinability of Kluttz with Alden and Citta

Applicant directs the Examiner to pages 17-19 of the 9/25/2008 Amendment. In this section, Applicant discusses Alden and Citta in detail, and demonstrates how Alden and Citta are each directed to transport-layer encryption.

Applicant goes on to describe how Kluttz, on the other hand, is directed to encrypting a stored file or document (e.g., see Page 20 of the 9/25/2008 Amendment). Referring to Figures 3 and 4 of Kluttz, Kluttz teaches partitioning a document into multiple portions, and applying a different level of encryption to each portion. Portions associated with “higher” level encryption are encrypted with a higher-level specific encryption key, as well as any “lower” level encryption keys. Thus, more confidential material is protected by both the higher level encryption key as well as all lower level encryption keys. As will be appreciated by one of

Reply to Office Action dated December 15, 2008

ordinary skill in the art, the encryption of Kluttz is directed to a file storage protocol executed at the application layer, and not at a transport layer (as in Alden and Citta).

Even assuming for the sake of argument that one of ordinary skill in the art could find some motivation to combine Alden, Citta and Kluttz, the alleged combination would not result in the claimed invention. The methodologies associated with encryption of file storage documents, such as MS Word documents, MS Excel documents, etc., cannot simply be imported into the transport layer for encrypting TCP/IP packets. As will now be described in detail, there are fundamental differences between encryption performed at the file storage layer, or “application layer”, and encryption performed at the TCP/IP layer, or “transport layer”.

In Alden, the pseudo network adapter 259 is essentially “dumb”. In other words, the pseudo network adapter 259 does not have any special knowledge regarding any particular packet that is encrypted/encapsulated, but rather simply encrypts/encapsulates any received packets. As is known in the art, in preparing a file document for transmission at the transport layer, the file document is broken up into payload-portions in a plurality of packets, such as TCP/IP packets, for transmission. The pseudo network adapter 259 does not evaluate the “content” of any packets, nor does the pseudo network adapter 259 evaluate or even consider the “document” from which individual packets were generated. Such actions simply are not performed at the transport layer.

Likewise, in Citta, the address of a transport-layer packet is used to determine what type of content is being received at the subscriber terminal (e.g., HBO, Showtime, etc.), and the address keys are used to decrypt that content at the subscriber terminal. The subscriber is not aware of what the content is that is being sent, but simply attempts to decode based on its personal address key, which is associated with the subscriber’s permissions. If the packet cannot be decoded it is simply discarded.

Accordingly, Kluttz's method of partitioning a storage file document into different portions associated with different levels of encryptions makes no sense at the transport layer, nor is there any comparable transport layer operation that could be achieved based on the teachings of Alden and/or what is known in the art. In other words, how could a document be partitioned when the pseudo network adapter 259 of Alden, or the subscriber in Citta, only has knowledge of an individual packet with no knowledge of that packet's association with any particular document? How could the pseudo network adapter 259 in Alden, or the subscriber in Citta, associate that packet with a corresponding portion of a document that is associated with a given level of security/encryption? Many more questions could be raised regarding this alleged "obvious" implementation or combination.

Instead of combining the references in the manner alleged by the Examiner, Applicant respectfully submits that a much more likely combination of Alden, Citta and Kluttz would simply be to (i) encrypt a file storage document at the application layer as indicated by Figure 2 of Kluttz and (ii) if it is determined to send the file storage document to another entity, to break up the file storage document into individual packets as is known in the art and process the individual packets through the pseudo network adapter 259 as described by Alden. At the receiving end, a subscriber would receive the packet, as in Citta, and attempt to decode/decrypt the packet based on its address key. In other words, because Alden or Citta and Kluttz deal with encryption at different layers, their processes would be applied separately, and not meshed together in the manner suggested by the Examiner. Applicant notes that the claims would not read upon Kluttz, Citta and Alden combined in this manner.

1. Applicant respectfully requests a clarification from the Examiner regarding the last sentence on Page 4 of the 12/15/2008 Final Rejection

The Examiner states “[t]herefore, given the limitation ‘sequential code’ its broadest interpretation (MPEP 2111), the following references are used for the teaching of ‘sequential code’” (e.g., see Page 4 of the 12/15/2008 Final Rejection). The Examiner goes on to describe portions of the disclosure of Perlman, Barnett and Kluttz (e.g., see Page 5 of the 12/15/2008 Final Rejection).

Regarding Barnett, Applicant at least understands how the Examiner is attempting to read “sequential code”. However, Applicant is less sure regarding how this term is intended to be read regarding Perlman and/or Kluttz, or how the reading of “sequential code” upon these references affects the arguments of the Examiner. For example, while Applicant cannot be sure, it appears the Examiner reads “sequential code” upon Perlman’s keys 32 and Kluttz’s encryption keys 72. However, as the Examiner has not actually rejected the claims based on Perlman or Kluttz in the manner implied in this section in the Response to Arguments section of the 12/15/2008, Applicant will refrain from further comment until the Examiner reevaluates Applicant’s arguments presented herein.

Further, even if Kluttz and/or Perlman were to include some teachings upon which “sequential code” could read, the Graham v. John Deere Co., 383 U.S. 1 (1966) factors related to whether it would be obvious to combine these particular portions with Alden and Citta have not been addressed by the Examiner. Also, Applicant does not claim a “sequential code” in a vacuum, but also claims “encapsulating said first encrypted data frame in a first transport frame, said first transport frame comprising a first portion and a second portion of said first sequential code” as recited in independent claim 1, for example (emphasis added).

SUMMARY

Since the Examiner has maintained his rejection of claims 1-28 and 33-34 under 35 U.S.C. § 102 and 103 as noted above, Applicant once again traverses these rejections. Applicant expressly maintains the reasons from the prior responses to clearly indicate on the record that Applicant has not conceded any of the previous positions relative to the maintained rejections. For brevity, Applicant expressly incorporates the prior arguments presented in the September 25, 2008 response without a literal rendition of those arguments in this response.

For at least the foregoing reasons and the reasons set forth in Applicant's response of September 25, 2008, it is respectfully submitted that claims 1, 4, 7, 10, 13, 17, 21 and 25 are distinguishable over the applied art. The remaining dependent claims are allowable at least by virtue of their dependency on the above-identified independent claims. See MPEP § 2143.01. Moreover, these claims recite additional subject matter, which is not suggested by the documents taken either alone or in combination.

CONCLUSION

In view of the foregoing amendments and remarks, it is respectfully submitted that the application is in condition for allowance. If the Examiner believes that any additional changes would place the application in better condition for allowance, the Examiner is invited to contact the undersigned attorney, at the telephone number listed below.

Deposit Account Authorization

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any fees or overpayments that may be due with this response to Deposit Account No. 17-0026.

Respectfully submitted,

Dated: February 13, 2009

By: 

Raphael Freiwirth
Reg. No. 52918

QUALCOMM Incorporated
Attn: Patent Department
5775 Morehouse Drive
San Diego, California 92121-1714
Telephone: (858) 658-5787
Facsimile: (858) 658-2502

Attachment(s): None